








NO THREAT FOUND













File Name: AVSMeter.exe
File Type: PE32 executable (console) Intel 80386, for MS Windows
SHA1: 644a4e130b25db027734084daea5698967afdf32
MD5: d171919c4fc0313d66d1c76ccc7f7059
First Seen Date: 2020-11-25 15:21:46 UTC
Number of Clients Seen: 1
Last Analysis Date: 2020-11-25 15:21:46 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Valkyrie Automatic Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2020-11-25 15:21:46 UTC	No Match 
Static Analysis Overall Verdict	2020-11-25 15:21:46 UTC	No Threat Found 
Precise Detectors Overall Verdict	2020-11-25 15:21:46 UTC	No Match 
File Certificate Validation		Not Applicable 

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean 
Non-ascii or empty section names detected	Clean 
Illegal size of optional Header	Clean 
Packer detection on signature database	Unknown 
Based on the sections entropy check! file is possibly packed	Clean 
Timestamp value suspicious	Clean 
Header Checksum is zero!	Suspicious 
Entry point is outside the 1st(.code) section! Binary is possibly packed	Clean 
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean 
Anti-vm present	Suspicious 
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean 
TLS callback functions array detected	Clean 

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise NI Detector 3	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2020-11-25 15:21:21 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2020-11-25 15:21:21 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5E998379 [Fri Apr 17 10:22:49 2020 UTC]
Debug Artifacts	
Entry Point	0x426b13 (.text)
Exifinfo	[object Object]
File Size	433152
File Type Enum	6
Imphash	f2a46f83a176cf8c104145984a949d56
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	1
Product Version	2.9.9.1
Product Name	AVSMeter
File Version	2.9.9.1
Comments	AVSMeter - Avisynth Script Testing
File Description	AVSMeter
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	b6ec8a169a1af4bdc694a00600780f6a9c6e2f03d8efb1bf2cf416969bffc84
Ssdeep	6144:Ght/m/ljHk39ygNTzmVF3QAnmSwe6DQL5EqJM:GhFqNHkNVzUbnmSwe6eEqO
Trid	42.2,Win32 Executable MS Visual C++ (generic),37.3,Win64 Executable (generic),8.8,Win32 Dynamic Link Library (generic),6,Win32 Executable (generic),2.7,Generic Win/DOS Executable

File Paths



FILE PATH ON CLIENT	SEEN COUNT
C:\Program Files\Hybrid\32bit\AVSMeter.exe	1

PE Sections



NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x391c7	0x39200	6.55020080003	a64996d1ab47ececdbb6767e3f5b82b3
.rdata	0x3b000	0x242a2	0x24400	4.9892665906	3eb4e13cb4c67fc799f9a94845bb82d7
.data	0x60000	0x3c84	0x1a00	3.95592403805	0b8c21856bb80cdc8779701ce64d4760
.rsrc	0x64000	0x4810	0x4a00	5.86623363028	621f582a68953ef82bed24ae578901bf
.reloc	0x69000	0x5c92	0x5e00	6.01894721498	3975c1f0753b1849b457e5e6c2dd5bcb